**IN THE UNITED STATES DISTRICT COURT**
**FOR THE EASTERN DISTRICT OF OKLAHOMA**

| | |
|---|---|
| **UNITED STATES OF AMERICA,**<br><br>***Plaintiff*,**<br><br>**v.**<br><br>**SILVIA VERONICA FUENTES,**<br><br>***Defendant.*** | **Case No. CR-21-358-RAW** |

**UNITED STATES' OBJECTIONS TO MAGISTRATE JUDGE'S FINDINGS AND RECOMMENDATIONS (DOC. 147)**

CHRISTOPHER J. WILSON
United States Attorney

*/s/ T. Cameron McEwen*
T. Cameron McEwen,
AL Bar #7161R67M
Assistant United States Attorney
520 Denison Avenue
Muskogee, OK 74401
(918) 684-5150
Cameron.McEwen@usdoj.gov

October 1, 2024

# TABLE OF CONTENTS

## TABLE OF AUTHORITIES

**Cases**

**Statutes**

**UNITED STATES' OBJECTIONS TO MAGISTRATE JUDGE'S FINDINGS AND RECOMMENDATIONS (DOC. 147)**

Comes now the United States of America, by and through United States Attorney Christopher J. Wilson and Assistant United States Attorney T. Cameron McEwen and submits the following objections to the Magistrate Judge's Findings and Recommendation (Doc. 147). The United States respectfully requests this Court not adopt the Magistrate Judge's Findings and Recommendation and deny Defendant's Opposed Motion to Suppress Evidence Obtained by *Google "Geofence" Search Warrant* and Brief in Support (Doc. 39). Magistrate Judge Jason A. Robertson's interpretation of *Carpenter v. United States*, 585 U.S. 296 (2018), his reliance on *United States v. Smith*, 110 F.4th 817 (5th Cir. 2024), and his conclusion that the good-faith exception does not apply in this case are wrong and should be rejected by this Court.

In support of its requests, the United States asks the Court to consider the facts and argument in the United States' Response to Defendant's Motion to Suppress Evidence Obtained by Google "Geofence" Search Warrant and Brief in Support (Doc. 45), the Proposed Findings of Fact and Conclusions of Law Regarding Defendant's Motion to Suppress (Doc. 131), and Response to Defendant's Finding of Fact and Memorandum of Law in Support of Defense Motion to Suppress Evidence (Doc. 132), as well as the following objections.

**OBJECTIONS**

**I. The Magistrate Judge incorrectly found Defendant had a reasonable expectation of privacy in the location information sought by the Google geofence warrant and this Court should follow the precedent set forth by the Fourth and Eleventh Circuits.**

In his Findings and Recommendation, Magistrate Judge Jason A. Robertson incorrectly found Defendant had a reasonable expectation of privacy, under *Carpenter* and *Smith*, in the location information that the government obtained from Google. The Magistrate Judge's Findings and Recommendation should be rejected by this Court.

To assert a Fourth Amendment claim, a defendant must demonstrate "a legitimate expectation of privacy in the invaded place." *Rakas v. Illinois*, 439 U.S. 128, 143 (1978). To establish a legitimate privacy expectation, a defendant must demonstrate that his or her conduct exhibits "an actual (subjective) expectation of privacy," showing that "he seeks to preserve something as private." *Smith v. Maryland*, 442 U.S. 735, 740 (1979) (brackets and citation omitted). A defendant must further demonstrate the expectation is "one that society is prepared

to recognize as 'reasonable.'" *Ibid*. (citation omitted). "[D]efendants always bear the burden of establishing that the government violated a privacy interest that was protected by the Fourth Amendment." *United States v. Sheffield*, 832 F.3d 296, 305 (D.C. Cir. 2016). "Without a reasonable expectation of privacy, a Fourth Amendment search does *not* occur." *Stewart v. Evans*, 351 F.3d 1239, 1243 (D.C. Cir. 2003) (internal quotation marks and citation omitted). Here, Defendant lacked a reasonable expectation of privacy in her location on a public roadway over a brief four-minute period.

**A. Defendant lacks a reasonable expectation of privacy under *Carpenter* in the Google records.**

The Supreme Court has long recognized "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith*, 442 U.S. at 743-744. This includes business records of banks, *see United States v. Miller*, 425 U.S. 435, 440-443 (1976), and pen-register records of telephone numbers, *see Smith*, 442 U.S. at 742-744. Under this third-party doctrine, a bank or phone customer "assume[s] the risk that the company w[ill] reveal [the information] to the police." *Id.* at 744.

In *Carpenter*, however, the Supreme Court held this doctrine did not apply to the government's collection of at least seven days' worth of cell-tower location information from a cellular provider. 585 U.S. at 310 & n.3; 311 (noting that the government accessed 127 days of data). Although cell-tower records are created and maintained by third-party carriers, *id*. at 313, the Court "decline[d] to extend *Smith [v. Maryland]* and *Miller* to cover the[] novel circumstances" at issue, *Id*. at 309. The Court emphasized "the unique nature of cell phone location records" which provide "a detailed and comprehensive record of the person's [physical] movements" resulting in "near perfect surveillance, as if [the government] had attached an ankle monitor to the phone's user." *Id*. at 309, 312. The Court thus held the government's collection of cell-tower records documenting a particular phone's location over an extended period invades the user's reasonable expectation of privacy. *Id*. at 313.

In doing so, the Court emphasized the information in *Carpenter* was "not about 'using a phone' or a person's movement at a particular time," but instead implicated "a detailed chronicle of a person's physical presence compiled every day, every moment, over several years." 585 U.S. at 315. The Court further stated its holding was "a narrow one" and did not cover "tower dumps" where the government seeks "a download of information on all the

devices that connected to a particular cell site during a particular interval." *Id*. at 316. *See also United States v. Adkinson*, 916 F.3d 605, 611 (7th Cir. 2019) (stating that *Carpenter* "did not invalidate warrantless tower dumps (which identified phones near *one location* (the victim stores) at *one time* (during the robberies)).

Under *Carpenter*'s reasoning, the Google geofence warrant here did not infringe upon Defendant's reasonable expectation of privacy because it did not seek information that comprehensively chronicled her movements. Rather, the data revealed the presence of the defendant's phone on a public roadway over a brief four-minute period. Society has long accepted that type of surveillance capacity—where law enforcement monitors a suspect "for a brief stretch"—as reasonable. *Carpenter*, 585 U.S. at 310. *See also United States v. Chatrie*, 107 F.4th 319, 334 (4th Cir. 2024) ("[A]ccess to a person's short-term movements does not invade his reasonable expectation of privacy."). It was not the sort of "all-encompassing record of the holder's whereabouts" and "intimate window into a person's life" that concerned the Court in *Carpenter*, 585 U.S. at 311. *See United States v. Lauria*, 70 F.4th 106, 129 n.12 (2d Cir. 2023) ("*Carpenter*'s ruling gives no reason to doubt that law enforcement officers lawfully could have obtained more limited cell tower information—for example, information simply telling whether [the defendant's] cell phone was in the vicinity of the Mahopac store at or near the time of the robbery—without need to show probable cause."); *Leaders of a Beautiful Struggle v. Baltimore Police Dep't*, 2 F.4th 330, 341 (4th Cir. 2021)(en banc) (explaining that *Carpenter* does not govern "short-term tracking of public movements—akin to what law enforcement could do prior to the digital age")(internal quotation marks and brackets omitted).

Indeed, after *Carpenter*, courts have held the government may obtain limited location information of the type at issue here without implicating the Fourth Amendment. The Fourth and Eleventh Circuits have held the government did not conduct a Fourth Amendment search when obtaining limited geofence-location data from Google. Both circuits distinguished *Carpenter* on the ground that a defendant lacks a reasonable expectation of privacy in a discrete period of location-history data collected by Google. *See United States v. Davis*, 109 F.4th 1320, 1330 (11th Cir. 2024) (no reasonable expectation of privacy in location data at six locations for 40-50 minutes); *Chatrie*, 107 F.4th at 330-331 (no reasonable expectation in two hours of location data). The Seventh Circuit has similarly found no reasonable expectation of privacy in location records "where the officers only collected real-time

[cell-site location information] for a matter of hours while the suspect travelled on public roadways." *United States v. Hammond*, 996 F.3d 374, 392 (7th Cir. 2021). Other circuits have reached similar conclusions in related contexts. *See, e.g.*, *Sanchez v. Los Angeles Dep't of Transp.*, 39 F.4th 548, 559-561 (9th Cir. 2022) (e-scooter location data).

As these decisions illustrate, *Carpenter* does not apply here because the government obtained location information from Google covering only a discrete location at a discrete time. The tailored nature of the location information in this case—a brief four-minute period on a public roadway confined to a location only on the public roadway—underscores that conclusion.

Contrast this case with the 127 days of cell-tower location information at issue in *Carpenter*. Such data "provides an intimate window into a person's life, revealing not only his particular movements, but through them his familial, political, professional, religious, and sexual associations." 585 U.S. at 311 (internal quotation marks and citation omitted). It might specifically divulge the person's presence at "private residences, doctor's offices, political headquarters, and other potentially revealing locales" that hold the "'privacies of life.'" *Id.* (internal quotation marks and citation omitted).

No such disclosure risk is present in the limited location data obtained in this case. Because of the tailored geographic and temporal boundaries, "the geofence warrant here did not seek data from [the defendant's] home or any other area in which [the defendant] had a reasonable expectation of privacy." *Davis*, 109 F.4th at 1330. This distinction further explains why the defendant in *Carpenter* had a reasonable expectation of privacy in the location data, but this Defendant does not.

**B. Defendant also lacks a reasonable expectation of privacy in the Google location information because she voluntarily disclosed it.**

Defendant voluntarily disclosed her location to Google. *See* Government's Suppression Hearing Exhibit 24 at pgs. 8-9, ¶19 and footnote 4; and Exhibits 25 and 26; Suppression Hearing Transcript at pgs. 192-194, lines 20-25, 1-25, and 1-13. And because "an individual has a reduced expectation of privacy in information knowingly shared with another," *Carpenter*, 585 U.S. at 314, the defendant lacked a reasonable expectation of privacy in this location information. Here, Defendant created a Google account, linked it to her phone, and voluntarily disclosed her location information to Google.

Google offers an optional Location History feature that "allows Google to track a user's location while he carries his mobile devices," which, in turn, allows the user to "obtain personalized maps and recommendations, find his phone if he loses it, and receive real-time traffic updates." *Chatrie*, 107 F.4th at 322. "If a user opt[ed] in, Google ke[pt] a digital log of his movements and store[d] this data on its servers." *Chatrie*, 107 F.4th at 322. To use Google location services, a user has to opt-in to Location History and enable location reporting in order for that usage to be recorded. S*ee Chatrie*, 107 F.4th at 332 ("Location History is *off by default* and can be enabled only by a user's affirmative act."); *see also* Government's Suppression Hearing Exhibit 20 at pg. 5, ¶¶9-11; Suppression Hearing Transcript at pgs. 187-192, lines 8-25, 1-25, 1-25, 1-25, 1-25, and 1-19. A user also maintained the ability to review or delete his Location History information at any time. *See Chatrie*, 107 F.4th at 323. By affirmatively opting in to Location History, Defendant "knowingly and voluntarily expose[d] [her] Location History data to Google," *Chatrie*, 107 F.4th at 331, and "'assume[d] the risk'" that Google would turn that information over to third parties, *id*. at 332 (citation omitted).

Given these features, Defendant's voluntary disclosure of her location information to Google is the modern-day equivalent of the deposit slip in *Miller* showing that a customer deposited money into an account at a particular bank on a particular date, or the pen register in *Smith v. Maryland* showing that a person dialed a particular number on a particular date from the customer's home-telephone line. *See Chatrie*, 107 F.4th at 331 ("A record of a person's single, brief trip is no more revealing than his bank records or telephone call logs."). Defendant lacks a reasonable expectation of privacy in such information.

*Carpenter* confirms this conclusion. There, the Supreme Court reasoned the "[c]ell phone location information [at issue] is not truly 'shared'" by the user with his cellular provider. 585 U.S. at 315. Rather, "a cell phone logs a cell-site record by dint of its operation." *Id*. The location information stored at Google is different. As just explained, Defendant engaged in an "affirmative act" to use the Location History function and share her whereabouts with Google. *See id*.

An account holder like Defendant also had a ready "way to avoid leaving behind a trail of location data." *Carpenter*, 585 U.S. at 315. She could turn off the Location History setting for her Google account or disable location reporting for a particular device. She could also delete her Location History information stored by Google. "That two-thirds of active

Google users have not enabled Location History" dispels any notion Defendant's "decision to opt in was … involuntary."[1] *Chatrie*, 107 F.4th at 331. "The third-party doctrine therefore squarely governs" the location information stored at Google and the defendant "cannot now claim to have had a reasonable expectation of privacy in [it]." *Id*. at 332.

### C. The Fifth Circuit's analysis in *Smith* is unpersuasive and, in any event, not applicable to this Google geofence warrant.

The Fifth Circuit in *United States v. Smith*, 110 F.4th 817 (5th Cir. 2024), recently held that two defendants had an expectation of privacy under *Carpenter* in their location histories collected from Google. Here, the Magistrate Judge incorrectly relied on this decision in his Findings and Recommendation, and this Court should decline to follow that decision.

#### 1. *Smith* is wrong.

The geofence warrant in *Smith* specified a 98,000 square-meter area around a rural Mississippi post office where a postal-service driver had been brutally assaulted and robbed. 110 F.4th at 820, 826. Through a three-step process, the warrant sought three hours of location data (including data outside the specified area) and identity information for devices present within the specified area during the hour of the robbery. *Id.* at 827. Law enforcement subsequently obtained subscriber information for three devices; that information identified two of the assailants. *Id*. at 828.

The Fifth Circuit held the two assailants had a reasonable expectation of privacy in the location information under *Carpenter* and, therefore, Fourth Amendment standing to contest the warrants. *Smith*, 110 F.4th at 836. The court reasoned that "even a snapshot of precise location data … 'can expose highly sensitive information—think a visit to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip

[1] In his Findings and Recommendation, the Magistrate Judge stated that "[i]n 2018, it was estimated that approximately 592 million users had Location History activated on their Google account and the step one parameters requires a search of all of these accounts for time and geographic compliance." Doc. 147 at pg. 14. The suppression hearing record does not support this finding. According to the testimony and exhibits submitted at the hearing, out of the 592 million accounts in Google's Sensorvault database in 2018, only approximately one-third of the Google users had Location History enabled on their accounts; thus, only one-third of the 592 million accounts had Location History activated on their Google account. *See* Suppression Hearing Transcript at pgs. 213-215, lines 12-25, 1-25, and 1-21; Defendant's Suppression Hearing Exhibit A1-6 at pg. 24, ¶3.

club, the criminal defense attorney, the by-the-hour-motel, the union meeting, the mosque, synagogue or church, or the gay bar.'" *Id*. at 833 (internal quotation marks, brackets, and citation omitted). The data also "can easily follow an individual into areas normally considered some of the most private and intimate, particularly residences." *Id*. The court viewed this functionality as "invasive for Fourth Amendment purposes" because the tracking occurs "regardless of whether a particular individual is suspicious or moving within an area that is typically granted Fourth Amendment protection." *Id*. at 834.

The Fifth Circuit acknowledged that Google "users opt in to having their Location History monitored," but rejected the contention that this extinguished their privacy interests under the third-party doctrine. *Smith*, 110 F.4th at 835. The court reasoned that "electronic opt-in processes are hardly informed and, in many instances, may not even be voluntary" because "users are bombarded multiple times with requests to opt in across multiple apps," those prompts "typically innocuously promise app optimization," and users likely fail to realize that they will "provid[e] their location information to Google in a way that will result in the government's ability to obtain … their precise geographical location at virtually any point in the history of their use of the device." *Id*. (internal quotation marks and citation omitted).

This Court should reject the Fifth Circuit's analysis as unpersuasive for two reasons. First, the geofence warrant in *Smith* did not provide "a detailed and comprehensive record of the person's [physical] movements" resulting in "near perfect surveillance, as if [the government] had attached an ankle monitor to the phone's user." *Carpenter*, 585 U.S. at 309. The warrant instead obtained information about the individuals "'using a phone' … at a particular time" in a particular rural Mississippi location. *Id*. at 315. The Supreme Court in *Carpenter* made clear that its "narrow" holding did not encompass that circumstance. *Id*. at 316.

Second, the Fifth Circuit wrongly dismissed the third-party doctrine's application. The court acknowledged that users must opt in to the location- history function, but questioned whether that opt-in was knowing and voluntary. The fact that two-thirds of Google users decline the function, *see Chatrie*, 107 F.4th at 331, undercuts the concern that the opt-in is illusory. And while some users may hurriedly select the opt-in when creating a Google account, *see Smith*, 110 F.4th at 836, the same situation assuredly arises when some bank customers quickly sign account-opening forms explaining how the bank will collect and

share their information. Those customers lack privacy expectations over their account information by virtue of "voluntarily convey[ing it to the bank[]." *Miller*, 425 U.S. at 442.

The Supreme Court's refusal to apply the third-party doctrine in *Carpenter* was tethered to a specific conclusion: that "carrying [a cell phone] is indispensable to participation in modern society" and "there is no way to avoid leaving behind a trail of location data." 585 U.S. at 315. The same cannot be said of Google's location-history function. It is not essential to participation in modern society; "[location history's] activation is unnecessary to use a phone or even to use apps like Google Maps." *Chatrie*, 107 F.3d at 331. Account holders can also turn the function off and delete their location histories whenever they want.

**2. *Smith*'s analysis also does not encompass the Google geofence warrant in this case.**

In any event, the Fifth Circuit in *Smith* made clear that its analysis applied to "the use of geofence warrants … *as described herein*." 110 F.4th at 820 [emphasis added]. The warrant at issue here is materially different.

In concluding that the defendants in *Smith* had a reasonable expectation of privacy in their location histories, the Fifth Circuit cited "the potential intrusiveness of even a snapshot of precise location data" and the possibility that the data could "follow an individual into areas normally considered some of the most private and intimate, particularly residences." 110 F.4th at 833. That concern appears to implicate the warrant in *Smith*, which had sought hours of location data for all devices present in the geofenced area that circled the robbery scene. The Google geofence warrant here, by contrast, sought no location data beyond a public roadway.

As noted, the geofence in this case aligned with specific parameters around a public roadway. This geographic separation between a public roadway and the various private locations cited by the Fifth Circuit in *Smith* negates the possibility that the geofence data here could have disclosed any private or sensitive location information. Accordingly, even if the two defendants in *Smith* had a reasonable expectation of privacy in their location information within the rural Mississippi area, Defendant here lacked a similar expectation in her location information on a public roadway.

## II. Defendant's Fourth Amendment challenge also fails on its merits because the Google geofence warrant articulated probable cause and was sufficiently particular.

In the Findings and Recommendation, the Magistrate Judge incorrectly found that the Google geofence warrant lacked probable cause and lacked particularity. Even assuming the information disclosed by Google implicated the defendant's privacy interests, the United States obtained a search warrant that complied with the Fourth Amendment. The Google geofence warrant was supported by probable cause and identified the records to be seized with sufficient particularity. Therefore, the Magistrate Judge's Findings and Recommendation should be rejected.

### 1. The Google geofence warrant affidavit established probable cause.

The probable-cause standard "is not a high bar," *District of Columbia v. Wesby*, 583 U.S. 48, 57 (2018) (citation omitted). When approving a search warrant, the magistrate judge need only determine whether "reasonable inferences" from the evidence described in the warrant application establish a "fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238, 240 (1983). Because the probable-cause standard deals not "with hard certainties, but with probabilities," *id*. at 231 (citation omitted), the facts presented to the magistrate judge need only "'warrant a person of reasonable caution in the belief' that contraband or evidence of a crime is present," *Florida v. Harris*, 568 U.S. 237, 243 (2013) (brackets and citation omitted).

The Google geofence warrant affidavit in this case easily passes muster. Under the "Probable Cause" section of the affidavit, it reads:

> "21. On March 18, 2021, at 21:54 hours, a fatal traffic collision occurred at the intersection of U.S. Highway 62 and South 460 Road in Cherokee County, Oklahoma. This location is within the Eastern District of Oklahoma and within the definition of "Indian Country" as it occurred within the boundaries of the Cherokee Nation reservation.
>
> 22. Affiant and other Troopers of the Oklahoma Highway Patrol were dispatched to the scene. Based on our observation of evidence at the scene, including debris from a vehicle, and speaking to witnesses, investigators determined that a female later identified as Jacklyn Dobson, was travelling southbound on South 460 Rd. on her bicycle and was attempting to cross U.S. 62, when she was struck by an unknown vehicle travelling westbound on U.S. 62. Dobson was assisted by another motorist until she was transported by air

ambulance to St. John Hospital in Tulsa. She later died from her injuries. Dobson was confirmed as a member of the Cherokee Nation.

23. The location of the collision is a rural, four-lane highway separated by an unimproved median. There are no traffic control devices. There are a small number of commercial businesses and residences located near the intersection. I was able to retrieve surveillance video from several nearby businesses. A review of the videos shows that the collision occurred at 21:54 hours and that shortly after the collision, the suspect vehicle pulled over to the shoulder of the highway a short distance from the collision. The suspect vehicle stopped for approximately 10 seconds before resuming westbound travel on U.S. 62 and leaving the scene. In the one-minute timespan after the collision, the videos show six other vehicles travelling through the collision area. Five of the six vehicles are travelling eastbound.

24. Based on my training and experience, as well as a review of professional literature, a vast majority of motorists not only own but use their smartphones while driving. In one of the largest and most comprehensive distracted driving studies to date, involving the collection and analysis of data from over 570-million trips driven by three million motorists over a three-month time period, drivers used their smartphones in 88 out of every 100 trips. Cameron Jahn, Largest Distracted Driving Behavior Study, Zendrive (Apr. 17, 2017), http://blog.zendrive.com/blog/distracted-driving/;Angie Schmitt, Study: Drivers with Smart Phones Use Them Almost Every Time They Drive, StreetsBlogUSA (Apr. 17, 2017), https://usa.streetsblog.org/2017/04/17/study-drivers-with-smart-phones-use-them-almost-every-time-they-drive. Despite legislative efforts and public awareness campaigns to curb cellphone use while driving, research suggests that the number of motorists who use their cellphones has been trending upward. See, e.g., Jeff Plungis, Drivers Still Can't Keep Hands Off Phones, Study Finds, Consumer Reports (Jan. 24, 2019), https://www.consumerreports.org/car-safety/distracted-driving-study-drivers-cant-keep-hands-off-phones (noting that in one study, the number of motorists using cellphones while driving increased 57 percent from 2014 to 2018).

25. Based on my training, experience, and a review of professional literature, a significant number of collisions occur as a result of distracted driving from a variety of sources, including cellphone use. See, e.g., Nat'l Highway Traffic Safety Admin., Distracted Driving 2018 (2020) available at https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/812926. Additionally, it has also been my experience that persons involved

> in a collision often use their cellphone immediately or shortly after a collision if not to call emergency services, then to call family members or friends."

*See* Government's Suppression Hearing Exhibit 8. Paragraphs 21 through 23 of the affidavit describe the relevant facts related to the investigation of the collision on U.S. 62 on March 18, 2021. *See id*. Paragraphs 24 and 25 illustrate how many people use cell phones while operating a vehicle and the effects of their use. *See id*. Additionally, paragraphs 7 through 20 go into great detail on how Google location services work with cell phones. *See id*.

Just because there was no evidence collected of the suspect driver possessing or using a cell phone at the time of the collision, does not mean probable cause could not be established through other facts and "reasonable inferences" that the driver of the vehicle likely possessed a cell phone at the time of the collision and Google location services were active on it at that time. *See* Doc. 147 at pg. 23. Furthermore, contrary to the Magistrate Judge's subjective belief, *see id.*, facts supporting the number or percentage of drivers who use cell phones while driving and the number of drivers who are involved in a collision because of cell phone use while driving are highly relevant to the issue at hand. These facts coupled with facts related to the investigation and an understanding of how Google location services work on cell phones presented more than enough evidence and "reasonable inferences" to establish a "fair probability that contraband or evidence of a crime will be found in a particular place[,]" namely, Google's records. *See Gates*, 462 U.S. at 238, 240.

Furthermore, "[s]earch warrants are not directed at persons; they authorize the search of places and the seizure of things." *Zurcher v. Stanford Daily*, 436 U.S. 547, 555 (1978) (internal quotation marks and brackets omitted). To that end, "valid warrants to search property may be issued when it is satisfactorily demonstrated to the magistrate that fruits, instrumentalities, or evidence of crime is located on the premises." *Id*. at 559. Warrant affidavits may accordingly establish probable cause to search a location for evidence of crimes by yet-to-be-identified suspects.

*Zurcher*'s facts illustrate this point. The Supreme Court approved a warrant to search a newsroom and seize photographs taken by a reporter of demonstrators assaulting a group of police officers because those photographs constituted material and relevant evidence showing the identity of the perpetrators. *Id*. at 551, 567-568. The court did so even though the warrant

affidavit contained no allegation that the reporter was in any way involved in the assault. *Id*. at 551. *Zurcher* thus confirms that law enforcement may obtain a warrant to search the premises of a third party for evidence identifying those present at a crime scene.

Additionally, in *Illinois v. Lidster*, 540 U.S. 419 (2004), the Supreme Court held police did not violate the Fourth Amendment when officers set up a roadblock to briefly seize all motorists at the scene of a hit-and-run. one week after that crime, for the primary purpose of locating witnesses. *Id.* at 423, 428. The Court held that the stop's objective — "to help find the perpetrator of a specific and known crime"—was valid. *Id*. at 427. It further reasoned that the roadblock was "appropriately tailored … to fit important criminal investigatory needs," and that the stops "interfered only minimally with liberty of the sort the Fourth Amendment seeks to protect." *Id.*

The same lesson holds here. If the Fourth Amendment permits brief physical stops without individualized suspicion of all persons traveling near the scene of a week-old crime to locate witnesses, it likewise permits the warrant-authorized collection of discrete location information for (but not physical seizure of) mobile devices present at the scene of a crime to locate the perpetrator(s) and witnesses of that crime.

Therefore, based on the foregoing, the Google geofence warrant established probable cause.

**2. The Google geofence warrant was sufficiently particular.**

"[T]he Fourth Amendment categorically prohibits the issuance of any warrant except one 'particularly describing the place to be searched and the persons or things to be seized.'" *Maryland v. Garrison*, 480 U.S. 79, 84 (1987). "By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit." *Id*. Here, the Google geofence warrant amply satisfies this requirement by specifying the particular property to be searched and records to be seized.

The Google geofence warrant delineated the records to be searched:

> 1. Location History data, sourced from information including GPS data and information about visible wi-fi points and Bluetooth beacons transmitted from devices to Google, reflecting devices that Google calculated were or could have been (as indicated by margin of error, *i.e.,* "maps display

radius") located within the geographical region bounded by the latitudinal and longitudinal coordinates, dates, and times below; and

2. identifying information for Google Accounts associated with the responsive Location History data.

- Date/Time Period: **03-18-2021 from 21:52 – 21:56 hours (CST)**

- Target Location: **Geographical area approximately 1000' by 170' and identified as a polygon defined by the following latitude/longitude coordinates (see below)**
  - **35.80815, -95.07356**
  - **35.80778, -95.07328**
  - **35.80686, -95.07652**
  - **35.80645, -95.07627**

Government's Suppression Hearing Exhibit 8, Attachment A.

The warrant also specifically identified what information should be disclosed by Google and seized via a three-step process:

1. Google shall query location history data based on the Initial Search Parameters specified in Attachment A. For each location point recorded within the Initial Search Parameters, and for each location point recorded outside the Initial Search Parameters where the margin of error (*i.e.*, "maps display radius") would permit the device to be located within the Initial Search Parameters, Google shall produce to the Government information specifying the corresponding unique device ID, timestamp, location coordinates, display radius, and data source, if available (the "Device List").

2. The Government shall review the Device List and identify to Google the devices about which it seeks to obtain Google account identifier and basic subscriber information. The Government may, at its discretion, identify a subset of the devices.

3. Google shall disclose to the Government identifying information, as defined in 18 U.S.C. § 2703(c)(2), for the Google Accounts associated with each device ID appearing on the Device List about which the Government inquires.

*Id*. at Attachment B.

This warrant did not authorize a "wide-ranging exploratory search[]" of Google's records. *Garrison*, 480 U.S. at 84. The search instead "constrained—both geographically and temporally—to the [crime] under investigation" that occurred on U.S. 62. *United States v. James*, 3 F.4th 1102, 1106 (8th Cir. 2021) (internal quotation marks omitted). The Google

geofence warrant sought location information for mobile devices traveling on U.S. 62, a public roadway, two minutes before and after the time of the collision. "[T]he period[s] w[ere] narrow and precise … with exact times listed." *Id*. "Given these specific limitations, the warrants were 'sufficiently definite' to eliminate any confusion about what the investigators could search." *Id*.

The warrant also incorporated "directions as to how the government must handle the … data." *In re: Information Stored at Premises Controlled by Verizon Wireless*, 616 F.Supp.3d 1, 11 (D.D.C. 2002). As explained above, the warrant directed Google to identify devices that were present within a two-minute period before and after the time of the collision. These constraints further "tailored the warrants to the greatest degree possible to obtain … data from the Service Providers to assist in identifying" individuals who were either involved in the collision or who witnessed the collision on U.S. 62 during the above-mentioned time period. *Verizon Wireless*, 616 F.Supp.3d at 12.

"[T]he particularity requirement seeks to assure that the[] searches … should be as limited as possible" with "nothing … left to the discretion of the officer executing the warrant." *United States v. Heldt*, 668 F.3d 1238, 1256 (D.C. Cir. 1981) (citation omitted). Here, the warrant did just that.

The *James* decision confirms this conclusion. The Eighth Circuit held that a series of cell-tower warrants used to solve a spree of robberies complied with the Fourth Amendment's particularity requirement. In so holding, the court stressed that the warrants "covered only the cellular towers near each robbery" for a "narrow and precise" period. 3 F.4th at 1106. Those limitations "eliminate[d] any confusion about what the investigators could search." *Id.*

The same is true here. The Google geofence warrant specifically sought location information for the area around collision at the time of the collision. That, in turn, limited the executing officers' discretion over the scope of the search.

The Fifth Circuit in *Smith* reached a contrary conclusion as to the Google geofence warrant there. It held that the warrant violated the Fourth Amendment's particularity requirement because it "force[d] the company to search through its *entire* database" of "all 592 million individual accounts" and because "law enforcement officials ha[d] *no idea* who they

[were] looking for, or whether the search w[ould] even turn up a result." 110 F.4th at 837. This reasoning should be rejected by this Court.

First, a geofence warrant does not command Google to search its entire database of accounts. It instead directs Google to identify the records in its possession corresponding to mobile devices detected to be within a designated geographic area at a particular time. This distinction is significant because, as Judge Contreras explained in *United States v. Rhine*, "the relevant [Fourth Amendment] question is not how Google runs searches on its data, but what the warrant authorizes the Government to search and seize." 652 F.Supp.3d 38, 82 (D.D.C. 2023). So long as the warrant defines those metrics with specificity, it authorizes a "search for the items described … anywhere in the [target location] where those items might be located." *United States v. Weaver*, 808 F.3d 26, 38 (D.C. Cir. 2015). Yet, under the Fifth Circuit's contrary approach, "many search warrants and most third-party subpoenas for protected records would be unconstitutionally overbroad because they necessarily would require the third party to search some group of records larger than those specifically requested, whether they reside in a file cabinet or on a server." *Rhine*, 652 F.Supp.3d at 82; s*ee also Chatrie*, 107 F.4th at 330 n.16 ("[A] search only occurs once the government accesses the requested information"); *Davis*, 109 F.4th at 1331 ("[E]ven if Google did have to search every single account when it sought to determine which devices were subject to the warrant, that search would not implicate [the defendant's] Fourth Amendment rights. The Constitution is not concerned with a private party's search of its own records.").

Second, Google's search of its entire database and initial production of location records produces only an anonymous identifier corresponding to a device detected to be within the geofence area. *See Rhine*, 652 F.Supp.3d at 68-69. Because this step "does not reveal the … owner's identity, address, phone number, or other personal information," this Court's case law holds that it is not an "intrusion on [his or her] constitutionally cognizable privacy interests." *Brennan v. Dickson*, 45 F.4th 48, 64-65 (D.C. Cir. 2022). That precedential principal undercuts the Fifth Circuit's conclusion that "geofence warrants fail at Step 1" because "they allow law enforcement to rummage through troves of location data from hundreds of millions of Google users." *Smith*, 110 F.4th at 837-838. If that initial step does not constitute a Fourth Amendment search, as *Brennan* dictates, the step cannot qualify as an impermissible general rummaging by law enforcement.

Third, the Fifth Circuit's criticism that law enforcement officers lack any "idea who they are looking for, or whether the search will even turn up a result" when seeking a geofence warrant misses the mark. 110 F.4th at 837 (emphasis omitted). The officers who obtained the search warrant in *Zurcher* similarly lacked concrete knowledge as to the identity of the perpetrators or whether the newsroom contained photographs displaying them. *See* 436 U.S. at 551. Because the warrant affidavit nonetheless articulated probable cause that the evidence of the crime might be found within the newsroom, the *Zurcher* warrant was valid. The same is true here. The Google geofence warrant affidavit articulated probable cause that the company's records contained evidence that would help identify the perpetrator(s) of a crime that occurred on U.S. 62 at the time of the collision. The Fourth Amendment's particularity requirement did not require the government to demonstrate any greater specificity as to identity of the perpetrator(s) or the likelihood that the target records would contain evidence of the crime.

Fourth, the dispute here involves the Fourth Amendment's particularity requirement for search warrants. The warrant here authorized the search of records at Google—not any location the government desired. The warrants also described with particularity the evidence to be seized: mobile- device location information tethered to a particular geographic location, date, time, and probable-cause showing. Google was also directed to perform the search and produce device identifiers, which would then, if applicable, be trimmed down based on additional parameters spelled out in the warrant. And ultimately, a federal magistrate judge reviewed and approved the warrant.

Lastly, in the Findings and Recommendation, the Magistrate Judge stated "[t]he Search Warrant executed in this case only required a two-step process to be followed" and "deviated from the three-step process established between Google and the Government in that the information produced under step one was not anonymized[2] and in a second step, the specific

[2] In the Findings and Recommendation, the Magistrate Judge's found that step one of the search warrant did not produce anonymized information. *See* Doc. 147 at pg. 16. The suppression hearing record does not support this finding. Both FBI Special Agent Jeremy D'Errico and Sarah Rodriguez from Google dispute this statement. *See* Suppression Hearing Transcript at pg. 173-185, lines 16-25, 1-25, 1-25, 1-25, 1-25, 1-25, 1-25, 1-25, 1-25, 1-25, 1-25, 1-25, and 1-5; *see also* Government's Suppression Hearing Exhibit 20, Sarah Rodriguez Affidavit, at pg. 3, ¶¶8-9. At the time of this Google geofence warrant, Google provided anonymized data to law enforcement via a device ID or a Reverse Location Obfuscation ID ("RLOI"). *See* Suppression Hearing Transcript

account information was then produced based entirely upon the Government's judgment as to which account user information was relevant to their investigation and would be produced by Google." Doc. 147 at pg. 16. The Magistrate Judge's findings are not supported by the record from the exhibits and testimony at the suppression hearing.

According to the testimony and exhibits during the suppression hearing, OHP Trooper and FBI TFO Dustin Thornton ("TFO Thornton") followed this three-step process when he executed the geofence warrant. In step one, Google produced geolocation data in an anonymized format, which revealed three devices inside the "geofence" boundary. *See* Government's Suppression Hearing Exhibits 10, 11, 12, 14, and 18; Suppression Hearing Transcript at pgs. 128-129, lines 6-25 and 1-18. The information produced from Google was anonymized because law enforcement had no way of identifying the individual(s) associated with the Device IDs without requesting additional data from Google. *Id*. One of these devices crossed through the geofence from 21:54:18 to 21:54:35 with three location datapoints within the geofence. *Id*. The timing and location of the datapoints of this device is consistent with the device travelling westbound on U.S. 62 at the exact moment of the collision and is consistent with the behavior of the suspect vehicle on video. *Id*.

In step two, TFO Thornton identified the accounts of interest, which was all three accounts, especially the account traveling westbound that started with the numbers 276 ("Suspect Account"). *See* Government's Suppression Hearing Exhibits 10 through 17; Suppression Hearing Transcript at pgs. 128-134, lines 19-25, 1-25, 1-25, 1-25, 1-25, 1-25, and 1-17. Based on his review, TFO Thornton elected to request the basic subscriber information for all three accounts because each account was linked to an individual that reasonably could be a suspect or witness in the investigation. *Id*. Just because TFO Thornton did not trim down the number of devices after review, does not mean that step two was not followed during the search warrant process. After review of the devices, TFO Thornton was within his right to request all devices that reasonably could be linked to a suspect or witness of the crime and this is exactly what he did in this case.

In step three, TFO Thornton requested and obtained the basic subscriber information for all three of the accounts from Google, including the Suspect Account, which belonged to Defendant. *See* Government's Suppression Hearing Exhibits 11 through 17. Law enforcement

---

at pg. 184-185, lines 6-25 and 1-5. Both mechanisms are anonymized. *Id*.

would not have been able to get this information any other way than by asking Google for it. *Id*. This information revealed that the Google account associated with the device traveling westbound at the time of the collision is account XXXXXXXX6595. *See* Government's Suppression Hearing Exhibit 15. The name associated with the account is "sXXXXX fXXXXXX" with an email of "XXXXXXXXXXX@gmail.com." *Id*. The account was created on March, 1, 2011, and uses a number of Google services and applications, including Web & App Activity, Gmail, Google Hangouts, iGoogle, Profiles, YouTube, Google Voice, Google Photos, Google Drive, Android, Google Calendar, Google Chrome Sync, Google Play Music, Google Docs, Google Play, Google Takeout, Location History, Google Cloud Print, Blogger, Google My Maps, Is In Family, Google Payments, Google Keep, G1 Phone Backup, Play Loyalty, Device Centric Auth, Android Device Console, Has Google One Membership Information. *Id*. Two cellphone numbers associated with the account are (XXX) XXX-1695 and (XXX) XXX-2760. *Id*. The account was still active, with the most recent login (at the time the data was compiled in response to the search warrant) being April 11, 2021. *Id*.

At the hearing, FBI Special Agent Jeremy D'Errico testified that a three-step process was used in this matter, which is in conjunction with the three-step process outlined by Ms. Sarah Rodriguez from Google in her affidavit. *See* Suppression Hearing Transcript at pgs. 172-173, lines 17-25 and 1-6; *see also* Government's Suppression Hearing Exhibit 20, Sarah Rodriguez Affidavit, at pgs. 2-4, ¶¶4-12. Special Agent D'Errico also testified that the second step does not require the government to narrow its request or ask for contextual data. *See* Suppression Hearing Transcript at pg. 173, lines 7-9. Additionally, he stated that a "unique device ID" is not unique across all of Google; it is only unique within an individual's account; and it is anonymized, which means law enforcement cannot identify who the device belongs to from the device ID number itself and can only identify who the device belongs to through requesting the information from Google. *See* Suppression Hearing Transcript at pg. 173-184, lines 16-25, 1-25, 1-25, 1-25, 1-25, 1-25, 1-25, 1-25, 1-25, 1-25, 1-25, and 1-5. Furthermore, Ms. Rodriguez's affidavit supports the fact that the device number is anonymized when she states, "[t]his deidentified 'production version' of the data includes a device number, the latitude/longitude coordinates and timestamp of the stored LH information, the map's display radius, and the source of the stored LH information (that is, whether the location was generated via Wi-Fi, GPS, or a cell tower)." *Id*. at

pgs. 182-184, lines 25, 1-25, and 1-5; Government's Suppression Hearing Exhibit 20, Sarah Rodriguez Affidavit, at pg. 3, ¶¶8-9.

Therefore, based on the foregoing, the Google geofence warrant in this case was sufficiently particular.

**III. The good-faith exception independently forecloses the relief sought by Defendant.**

In the Findings and Recommendation, the Magistrate Judge found the good-faith exception did not apply in this case because TFO Thornton "had actual knowledge of very little of the information provided to the neutral Magistrate Judge" and "[h]is attestation that the information provided was 'based upon his training and experience' was simply false." Doc. 147 at pgs. 25-26. The government respectfully disagrees and asks this Court to reject the Magistrate Judge's findings as to the good-faith exception and reject a finding that TFO Thornton's attestation "based upon his training and experience" was "simply false."[3]

The exclusionary rule is a "'judicially created remedy'" that is "designed to deter police misconduct." *United States v. Leon*, 468 U.S. 897, 906, 916 (1984) (citation omitted). The Supreme Court has explained that, in order to justify suppression, a case must involve police conduct that is "sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system" in suppressing evidence. *Herring v. United States*, 555 U.S. 135, 144 (2009); *see Davis v. United States*, 564 U.S. 229, 236-239 (2011).

*Leon* recognized a good-faith exception to the exclusionary rule in the context of search warrants: evidence should not be suppressed if officers acted in an "objectively reasonable" manner in relying on a search warrant, even if the warrant was later deemed deficient. *See* 468 U.S. at 922. *Leon* noted, for instance, that an officer's reliance would not be objectively reasonable when a warrant was "so lacking in indicia of probable cause" or "so facially deficient … in failing to particularize the place to be searched or the things to be seized … that the executing officers cannot reasonably presume it to be valid." *Id*. at 923 (internal quotation marks and citations omitted). "[T]he threshold for establishing" such a deficiency "is a high one, and it should be." *Messerschmidt v. Millender*, 565 U.S. 535, 547 (2012). "In the ordinary case, an officer cannot

[3] If this finding stands, every time TFO Thornton testifies in the future, this finding will need to be disclosed to defense counsel.

be expected to question the magistrate's probable-cause determination or his judgment that the form of the warrant is technically sufficient." *Leon*, 468 U.S. at 921.

The circumstances here fall within *Leon*'s good-faith exception. As in *Messerschmidt*, it would "not have been unreasonable—based on the facts set out in [the Google warrant] affidavit—for an officer to believe" that the requested information constituted evidence relevant to a crime occurring on U.S. 62 at the time of the collision. 565 U.S. at 551. As stated above, the affidavit articulated a fair probability that the individuals who were driving on U.S. 62 at or near the location of the collision at the time of the collision likely carried cell phones with them and that Google had location records identifying those individuals. The warrant also provided clear geographic and temporal limitations specifying the records to be searched and seized. Given these features, TFO Thornton could reasonably rely on the magistrate judge's conclusion that the warrant complied with the Fourth Amendment's probable-cause and particularity requirements.

Furthermore, when TFO Thornton sought the Google geofence search warrant in this case in March of 2021, this type of warrant was a new and novel investigative technique, and there were no judicial opinions analyzing them under the Fourth Amendment. The defendant even conceded during the suppression hearing that this type of warrant was novel at the time it was sought in this case. In *United States v. McLamb*, the Fourth Circuit rejected suppression in these types of circumstances. 880 F.3d 685 (4th Cir. 2018). The court held when considering a motion to suppress the fruits of a novel investigative technique, suppression was inappropriate where the investigating officer consulted with counsel and then sought a warrant:

> But in light of rapidly developing technology, there will not always be definitive precedent upon which law enforcement can rely when utilizing cutting edge investigative techniques. In such cases, consultation with government attorneys is precisely what *Leon's* 'good faith' expects of law enforcement. We are disinclined to conclude that a warrant is 'facially deficient' where the legality of an investigative technique is unclear and law enforcement seeks advice from counsel before applying for the warrant.

*Id*. at 691. Here, TFO Thornton followed the approach endorsed by *McLamb*. Because of the novelty of the search warrant, he consulted with an assistant United States attorney ("AUSA") about the search warrant prior to obtaining it and conferred with the AUSA throughout the entire search warrant process to ensure its accuracy and legality. Additionally, he received assistance from the AUSA in drafting the affidavit to insure it contained all necessary information. There is

nothing wrong with this. *See Smith v. Barber*, 316 F.Supp.2d 992, 1027 (D. Kan. 2004); *Snell v. Tunnell*, 920 F.2d 673, 693 (10th Cir.1990). TFO Thornton also sought and obtained a Google geofence search warrant from a United States magistrate judge. Thus, TFO Thornton did "precisely" what *McLamb* expects, and the good-faith exception precludes suppression here. In sum, he behaved reasonably for an investigator seeking to employ a new investigative technique.

In his Findings and Recommendation, the Magistrate Judge takes issue with TFO Thornton's "training and experience" because TFO Thornton received no formal training on Google geofence search warrants prior to seeking this search warrant, *see* Doc. 147 at pg. 25-26, but there is no indication in *McLamb* that the agents in that case had received training on darknet child pornography warrants prior to seeking the warrants. Indeed, such trainings may not exist when a new investigative technique first arises. *McLamb* calls for consultation with prosecutors and then seeking a warrant, not meeting a bureaucratic training requirement. Consulting directly with an AUSA or another law enforcement officer with prior experience in this type of search warrant is an effective form of training and experience, even if it is not officially categorized as such. Again, TFO Thornton did what *McLamb* calls for, and the good-faith exception therefore applies.

Moreover, by stating that TFO Thornton provided false information to the magistrate judge in his affidavit in the paragraph's that included the language "based on my training and experience," the Magistrate Judge is essentially saying TFO Thornton misled the magistrate judge by not being truthful about his training and experience related to Google, he intentionally omitted necessary facts related to Google that he should have included in the affidavit, and he misrepresented his knowledge about the surveys identified in the affidavit.

TFO Thornton did not intentionally mislead the magistrate judge nor did he provide false information to him. At the suppression hearing, TFO Thornton testified that his training and experience related to paragraphs 7 through 20 of the affidavit was limited to talking to other investigators that had done Google geofence search warrants and his personal knowledge in dealing with bluetooth. He did not try to hide anything from the Magistrate Judge nor did he testify that he no training and experience on the matter. His training and experience was just limited because of the novelty of the search warrant. Furthermore, he testified that in preparing the search warrant application, he worked directly with an AUSA, who physically drafted the affidavit. All of this is permissible, and it is reasonable for TFO Thornton to believe that the information that

the AUSA included in the affidavit related to Google or the studies in paragraphs 24 and 25 to be true and correct. Furthermore, FBI Special Agent D'Errico, an expert on Google geofences[4], confirmed at the suppression hearing that all substantive information contained in paragraphs 7 through 20 and the information in the studies in paragraphs 24 and 25 were true and correct. *See* Suppression Hearing Transcript at pgs. 148-150, lines 22-25, 1-25, and 1-19; pgs. 158-159, lines 22-25 and 1-2; and pgs. 239-240, lines 11-25 and 1-8. Therefore, any "reasonable inference" the magistrate judge gleamed from these paragraphs was based on true and correct facts.

Also, because of the novelty of these types of warrants at the time, TFO Thornton's training and experience would be expected to be limited or minimal. TFO Thornton took affirmative steps in consulting with an AUSA that assisted in drafting the affidavit in order to prepare a search warrant application that established probable cause. Thornton's affidavit was not knowingly false nor did Thornton display a reckless disregard for the truth. Any alleged or potential misstatements

[4] FBI Special Agent Jeremy D'Errico is a member of two specialty teams with the FBI. He is member of the FBI's Cellular Analysis Survey Team ("CAST") and its Child Abduction Rapid Deployment Team. *See* Suppression Hearing Transcript at pgs. 162-166, lines 16-25, 1-25, 1-25, 1-25, and 1-5; *see also* Government's Suppression Hearing Exhibit 21. CAST is a team that "specializes in conducting mobile device location, whether its through cell site location or call detail records or advanced timing events records or other information, such as records from Google Facebook or other providers that have location information." *Id*. Special Agent D'Errico has received over 300 hours of training in these areas, including advanced, certified training. *Id*. He also has specialized training in Google location history and has presented and instructed in this area. *Id*. He has presented on Google location history 10-15 times to hundreds of local, state, and federal law enforcement officers, as it is part of the curriculum for the FBI's basic historical cell site class. *Id*. He has also briefed his CAST team on Google location history and has presented once or twice on the subject at the FBI's annual conference. *Id*. Other training and experience he has received on Google location history includes attending webinars, reading about Google's patented technology in this area, reading Google's privacy policy, reading court filings related to this issue, testifying in court on the issue and experimenting or testing data related to Google geofence data to understand the intricacies of it. *Id*. He has been involved in over 100 cases involving Google location history and Google geofence warrants as a subject matter expert and has testified approximately 15-20 times as an expert on Google location history. *Id*. at pgs. 167-169, lines 12-25, 1-25, and 1. Special Agent D'Errico also has a bachelor's degree in computer science from James Madison University and a master's degree in security informatics from John Hopkins University. *Id*. at pg. 167, lines 4-11; *see also* Government's Suppression Hearing Exhibit 21. FBI Special Agent D'Errico's expertise is vastly greater than the defendant's expert in this case. In fact, other than testifying in court on behalf of defendant's, the defendant's expert has very minimal training and experience when it comes to Google geofence warrants. *See* Suppression Hearing Transcript at pgs. 33-108.

made by TFO Thorton pertaining to his training and experience are immaterial to the substance of the affidavit and do not affect the probable cause determination made by the magistrate judge.

Other federal courts have addressed this argument in the context of motions to suppress Google geofence search warrants. In those cases, the courts have not found bad-faith when an affiant is accused of misstating his training and experience in the search warrant affidavit. *See United States v. Smith*, 2023 WL 1930747 at *12 (N.D. Miss. February 10, 2023)[5] (motion to suppress denied even though affiant officers lacked prior training and experience related to Google geofence search warrants); *United States v. Carpenter*, 2023 WL 3352249 (M.D. Florida February 28, 2023) report and recommendation adopted by the District Court, 2023 WL 2910832 (M.D. Florida April 12, 2023) (motion to suppress denied even though affiant officer lacked training related to Google geofence search warrants; the affiant officer did not mislead the magistrate judge even though the affidavit included language such as "based on my training and experience, I know" before each Google-related fact in his affidavit).

As to TFO Thornton's knowledge of the surveys referenced in paragraphs 24 and 25 of his affidavit, he admitted to not reading them at the suppression hearing. He did not try to hide this fact from the Magistrate Judge during the hearing. However, this does not mean that he intentionally or recklessly omitted material information from the affidavit when attesting to the truthfulness of these paragraphs. Once again, the material information as to these paragraphs is true and correct. This was confirmed by FBI Special Agent D'Errico, who read and reviewed the surveys. Furthermore, because of TFO Thornton's extensive experience as an OHP Trooper, he knows the content in those paragraphs to be true without reading the surveys. He testified that he believes that the number of those who drive a vehicle with a cell phone is higher than 88 out of 100 based on his experience as a state trooper. Therefore, TFO Thornton did not intentionally mislead or recklessly omit material information from the affidavit by not reading the surveys identified in paragraphs 24 and 25.

Finally, the Fifth Circuit would apply the good-faith exception in this setting. After concluding that the disputed Google geofence warrant in *Smith* violated the Fourth Amendment's particularity requirement, it held that suppression was unwarranted because law

[5] This is the District Court ruling that ultimately resulted in the Fifth Circuit's decision in *United States v. Smith*, 110 F. 4th 817 (5th Cir. 2024). As noted below, the Fifth Circuit in *Smith* held that the good-faith exception applied to the Google geofence warrant and found the warrant valid. *Id*.

enforcement's actions were "'reasonable and appropriate'" "considering the novelty of the technique and the dearth of court precedent to follow." 110 F.4th at 840 (citation omitted). That tally provides strong confirmation that the officer who executed the Google warrant here reasonably relied on the magistrate judge's probable-cause and particularity determination. *See United States v. Workman*, 863 F.3d 1313, 1321 (10th Cir. 2017) (stating that, if eight federal judges were mistaken in upholding a particular warrant, investigators "could reasonably have made the same mistake"). Suppression is thus unwarranted in all respects.

## IV. Conclusion

Based on the foregoing arguments and authorities, the United States respectfully requests the Court not adopt the Magistrate's Findings and Recommendation and deny Defendant's Opposed Motion to Suppress Evidence Obtained by *Google "Geofence" Search Warrant* and Brief in Support. Furthermore, the United States specifically requests the Court find TFO Thornton's attestation that the information provided "based upon his training and experience" was not false.

Respectfully submitted,

CHRISTOPHER J. WILSON
United States Attorney

s/ *T. Cameron McEwen*

T. CAMERON MCEWEN
AL BAR # 7161-R67M
Assistant United States Attorney
520 South Denison
Muskogee, OK 74401
Telephone: (918) 684-5100
Cameron.McEwen@usdoj.gov

**CERTIFICATE OF SERVICE**

I hereby certify that on October 1, 2024, I electronically transmitted the attached document to the Clerk of Court using the ECF System for filing. Based on the records currently on file, the Clerk of Court will transmit a Notice of Electronic Filing to the following ECF registrants:

Juan L. Guerra, Jr., Attorney for the Defendant
Sidney Warren Thaxter, Attorney for the Defendant
Michael W. Price, Attorney for the Defendant

*s/ T. Cameron McEwen*
T. CAMERON MCEWEN
Assistant United States Attorney